

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

**Filed Under Seal Pursuant to Local Rule 157.6(a)**

I, Raymond T. Goergen, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since March 1998. Prior to becoming a Special Agent with the FBI, I was a Police Officer for seven and a half years with the Naperville Illinois Police Department. As an FBI Special Agent, I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), who is empowered by law to conduct investigations of and to make arrests for federal offenses including those enumerated in Title 18, United States Code, Sections 1341, 1343, 1028.

2. I am currently assigned to the FBI Boston Field Office, Bangor Resident Agency, and my duties and responsibilities include investigating matters involving financial crimes including, but not limited to, investigations of credit card fraud, wire fraud, and bank fraud. These investigations include the use of surveillance techniques, undercover activities, the interviewing of subjects and witnesses, and application and execution of search, arrest, and seizure warrants.

3. I have communicated with colleagues who have received training in the area of white collar crime offenses through the FBI. I am aware of the locations where evidence of white collar offences could be stored to include, but not limited to, all forms of electronic devices, including computers, portable media players, and tablets, as well as paper documents in the form of gift cards, bank statements, and loan payments, and have discussed and reviewed these materials with other law enforcement officers.

4. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at **32 Elmwood, Waterville, Maine**, as more particularly described in Attachment A of this affidavit (hereinafter the “target premises”), and any paper document, computers or other electronic devices contained therein, and to seize the items described in Attachment B of this affidavit.

5. This affidavit is intended to provide the facts necessary for a determination of probable cause. Based on my training and experience, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1341 (Mail fraud), 18 U.S.C. §§ 1343 (wire fraud); and 18 U.S.C. §§ 1028 (a)(7) (Fraud and related activity in connection with identification documents, authentication features and information), are presently located at the target premises. I am requesting authority to search the entire target premises, including the residential dwelling, persons in the dwelling, any storage unit assigned to that dwelling, any vehicles at the target premises and any computers and/or electronic devices found therein, for the items specified in Attachment B, hereto, which items constitute fruits, instrumentalities, and evidence of the foregoing violations.

6. The statements contained in this affidavit are based upon my investigation, information provided by other sworn law enforcement officers and other personnel specially trained in the seizure and analysis of computers and electronic media, and on my experience and training as a federal agent.

#### **DEFINITIONS**

7. Based on my training and experience, and information provided by fellow law enforcement professionals, I use the following technical terms (listed here alphabetically) to convey the following meanings in this affidavit and its attachments:

a. Computer: Computer is defined pursuant to 18 U.S.C. § 1030(e)(1), as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

b. Computer Hardware: Computer hardware consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, flash memory cards, CD-ROMS thumb drives and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

c. Computer passwords and data security devices: Computer passwords and data security devices consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain preset security functions when touched. Data security software or code may also encrypt,



compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

d. Computer-related documentation: Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

e. Computer Software: Computer software, as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

g. Internet Service Providers or ISPs: ISPs are businesses that enable individuals to obtain access to the Internet. ISPs provide their customers with access to the Internet using telephone or other telecommunications lines, provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs’ servers, remotely store electronic files on their customers’ behalf, and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, electronic mail transaction information, posting information, account application information, and other information both in computer data and written format.

h. Records, Documents and Materials: The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings, drawings, painting), photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as phonograph records, printing, typing) or electrical, electronic or magnetic form (such as tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as digital cameras, floppy diskettes, hard disks, CD ROMs, digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), Multi Media Cards (“MMC’s”), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, laptop computers or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

i. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook. A tablet is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks. Some tablets also come equipped with built in digital cameras.

j. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld electronic wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A

wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device. In addition to acting as wireless communication devices, wireless phones can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Such wireless telephones typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, video chatting, and participating in Internet social networks.

k. Green Dot: The **Green Dot Corporation** is an American financial technology and bank holding company headquartered in Pasadena, California. It is the world's largest prepaid debit card company by market capitalization. Green Dot is also a payments platform company and is the technology platform used by Apple Pay Cash, Uber, and Intuit. In 2001, the company pivoted to serving the “unbanked” and “underbanked” communities. Since its inception, Green Dot has acquired a number of companies in the mobile, financial, and tax industries including Loopt, AccountNow, AchieveCard, UniRush, and TPG. Green Dot Corporation is an issuer of prepaid MasterCard and Visa cards in the United States. These products are available at nearly 100,000 retail stores.



**PROBABLE CAUSE**

8. My investigation has revealed the following information relating to fraud and identify theft offenses:

a. Bethany A. Bing and Joseph L. Bing reside at 32 Elmwood Ave, Waterville, Maine. This information is based on the Maine Bureau of Motor Vehicle records which indicate Beth A. Bing, obtained her driver's license on August 8, 2018 and listed this as her residence. Additionally, per the criminal history of Joseph Bing, he is a registered sex offender with the Maine State Bureau of Identification. As of July 19, 2017, the 32 Elmwood address has been listed as his residence. A marriage certificate is on file with the Maine Department of Health and Human Services for a marriage between Beth and Joseph dated August 14, 2018.

b. On October 10, 2019, a 2016 red Nissan Rogue, bearing Maine registration 8361XR was observed at the target premises by law enforcement. The Nissan is registered to Beth A. Bing at the target premises. On October 30, 2019, a male matching the description of Joseph Bing was observed by law enforcement standing in the driveway of the target premises. The same Nissan Rogue was also present in the driveway at the target premises. Currently there are at least five vehicles registered with the State of Maine to Beth A. Bing at the target premises. BMV records show the following vehicles registered to Bing at 32 Elmwood Avenue in Waterville:

1. 2016 Nissan Rogue, red, Maine license plate number 8361XR
2. 2004 Dodge Ram, Silver, Maine license plate number 7084XQ
3. 2009 Chevrolet Malibu, white, Maine license plate number 1028VA

4. 2000 Acura TL, green, Maine license plate number 5336XL

5. 2002 Infinity I35, white, Maine license plate number 6152XK

c. Beginning no later than October 2018, WEX Inc. issued a series of alerts to Unity College regarding potential suspicious activity on College credit cards. WEX Inc. is a provider of payment processing and information management services to the United States commercial and government vehicle fleet industry. The company also provides services worldwide.

d. Unity College was alerted to suspicious activity regarding three credit cards. One (1) registered to John Hopkins, a professor at the college and two (2) registered to Bethany Bing. Bing served as the Business Office Coordinator working directly for the College Controller. Bing has been in the position for approximately 18 years. In this position, Bing was responsible for validating charges as authorized by the College.

e. Bing served as an administrator of the cards, as well as being responsible for seeing the credit card bills were paid. Bing was responsible to order all credit cards electronically from WEX Inc. for employees of the College via the internet. As the Business Office Coordinator she was not issued and had no need to have an employee credit card.

f. Employees of Unity College are required to fill out a procurement card application and have it approved by their supervisors and ultimately the Chief Business Officer. Once the forms are approved they are provided to Bing who in turn would order the credit cards electronically via WEX Inc.'s portal from a Unity College computer. WEX Inc. would then mail the credit cards in the names of the approved employees to Unity College where Bing would in turn provide the card to the employee.



g. Each month Bing would electronically receive the credit card statement from WEX Inc. for all credit cards authorized for the College and its employees. Bing would again log into WEX Inc. and initiate an Electronic Funds Transfer (EFT) from Bangor Savings Bank to WEX Inc. in the full amount of the balance.

h. Hopkins is reported to not have used his card since May of 2017. Bing was not authorized to have a card issued in her name. Credit card statements provided from WEX Inc. indicate Bing not only purchased items utilizing a credit card issued in her name, but is believed to have purchased items for herself and her husband Joseph Bing utilizing the credit card issued to Hopkins:

i. On October 30, 2018, a purchase was made utilizing a credit card in the name of John Hopkins from Delta Airlines for a ticket in the name of Joseph Bing. The purchase was made via delta.com in the amount of \$385.80.

j. On October 30, 2018, a purchase was made utilizing a credit card in the name of John Hopkins from Delta Airline for a ticket in the name of Beth Bing. The purchase was made via delta.com in the amount of \$385.80.

k. On October 30, 2018, a purchase was made utilizing a credit card in the name of John Hopkins from American Airline for a ticket in the name of Joseph Bing. The purchase was made in the amount of \$245.30.

l. On October 30, 2018, a purchase was made utilizing a credit card in the name of John Hopkins from American Airline for a ticket in the name of Beth Bing. The purchase was made in the amount of \$245.30.

m. On May 1, 2019, a purchase was made utilizing a credit card in the name of John Hopkins from Kennebec Auto Service for \$10.00.

- n. On May 2, 2019, a purchase was made utilizing a credit card in the name of John Hopkins from Green Dot Bank in the amount of \$533.70.
- o. On August 18, 2019, a purchase was made utilizing a credit card in the name of John Hopkins from Central Maine Power Company in the amount of \$300.00.
- p. On September 6, 2019, two purchases were made utilizing a credit card in the name of John Hopkins from Verizon Wireless. One in the amount of \$946.29 and the second in the amount of \$987.95.
- q. On September 9, 2019, a purchase was made using a credit card in the name of John Hopkins from Delta Airline for a ticket in the name of Joseph Bing. The purchase was made in the amount of \$900.00.
- r. On September 9, 2019, a purchase was made using a credit card in the name of John Hopkins from Delta Airline for a ticket in the name of Beth Bing. The purchase was made in the amount of \$900.00.
- s. On September 10, 2019, a purchase was made using a credit card in the name of John Hopkins at the Portland Maine airport in the amount of \$58.00.
- t. Between September 20-22, 2019, purchases were made using a credit card in the name of John Hopkins at the Foxwoods NIKE store in Mashantucket Connecticut, in the amount of \$69.87, the Hard Rock Foxwood , Mashantucket, CT in the amount of \$106.48, Michael Kors, Mashantucket CT in the amount of \$248.89, Coach, Mashantucket CT in the amount of \$348.80.
- u. Between September 20-22, 2019, purchases were made using a credit card in the name of Beth Bing, with last four digits 0041 at Foxwood Casino, Mashantucket Ct. There were four charges at the Foxwood Casino totaling \$12,011.96.

v. On September 26, 2019, a purchase was made using a credit card in the name of John Hopkins from Delta Airline for a ticket in the name of Joseph Bing. The purchase was in the amount of \$598.00.

w. On September 26, 2019, a purchase was made using a credit card in the name of John Hopkins from Delta Airline for a ticket in the name of Beth Bing. The purchase was in the amount of \$598.00.

x. The credit card statement for the month of September, 2019, lists the total purchase amount for a card issued to Beth Bing ending with the digits 0041, in the amount of \$38,015.75. The same statement lists one purchase on a card issued to Beth Bing, ending in 0017, in the amount of \$847.96, at the WinStar Hotel Tower on Thackerville OK, with an arrival date of September 27, 2019.

y. Between September 1, 2019, and October 2, 2019 there were approximately 15 purchases from Amazon market place utilizing the credit card issued to John Hopkins for approximately \$3,660.91.

z. The John Hopkins card was also used to make purchases at the Encore Casino in Boston from multiple times starting no later than July, 2019 and continuing through September, 2019. The card was also used to make purchases at Mohegan Sun Casino around in May and September 2019.

aa. Between about March 3, 2019 and about March 8, 2019, a series of purchases were made in and around Honolulu, Hawaii using a credit card in the name of John Hopkins. Mr. Hopkins confirmed to investigators that he had not been to Hawaii in over 15 years.



bb. On March 13, 2019, purchases were made using a credit card in the name of John Hopkins from Delta Airline for tickets in the name of Beth Bing, Joseph Bing, James Dostie, and Brianna Mayberry. According to Waterville Police, Brianna Mayberry is Beth Bing's daughter. Each of the tickets cost \$1,011.27. The same day, a charge on the same card was made for \$1,171.48 to Universal Orlando, and to Orbitz for \$2,020.05. On March 17 and 18, 2019, a series of charges were also made on the same card to Orlando area businesses.

cc. On October 10, 2019, an email was sent at 10:43 am from WEXMCFRAUD@wexinc.com to Beth Bing, bbing@unity.edu with the subject line as follows: Please verify the authorization activity for – BETH BING / 0017 (UNITY COLLEGE). The suspect authorization was for the charge of \$5,400.00 on October 10, 2019, at 10:58 am at the merchant EVI\*WINSTAR CASINO, and a second charge of \$305.50 on October 09, 2019 at 9:55 am at the merchant TWIN CITY TINT.

dd. On October 10, 2019, at 8:05 pm, a response was sent from [bbing@unity.edu](mailto:bbing@unity.edu) to [WEXMCFRAUD@wexinc.com](mailto:WEXMCFRAUD@wexinc.com) indicating the following: "These are valid charges." It should be noted this response was sent from a Verizon, Samsung Galaxy smartphone.

ee. On October 15, 2019, Beth Bing was placed on suspension pending the suspicious activity associated with credit cards in her name and the name of John Hopkins. Bing was escorted from Unity College. Located in Bing's office was a copy of an invoice from Kennebec Auto Service, Invoice number 85888 which was paid on October 14, 2019 in the amount of \$86.50 which was paid in cash. The work order was for a 2004 Dodge Ram, Maine registration 7084XQ, registered to Beth Bing at 32 Elmwood. This vehicle was seen at the target premises on November 3, 2019.

ff. Unity College has identified a total of approximately \$500,000 in unauthorized purchases on the Bing and Hopkins cards since 2017.

9. Based on the foregoing, I have probable cause to believe that Bethany Bing violated federal law relating to wire and mail fraud by purposefully engaging in a scheme to defraud Unity College of money, and that this scheme involved the use of wire transmissions, both in the use of the cards and in the sending of emails falsely claiming the charges were valid, and involved the use of mail in processing credit card applications and receiving invoices, and in receiving goods fraudulently purchased. I also have probable cause to believe that Bethany Bing violated Title 18, United States Code, Section 1028(a)(7), by using an account number assigned to John Hopkins in furtherance of these fraud activities, in a manner that was in and affecting interstate commerce.

#### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

10. As described above and in Attachment B, this application seeks permission to search for records that might be found on the target premises, in whatever form they are found. One form in which the records might be found is data stored on a computer, other electronic storage media like hard drives and/or USB thumb drives, and electronic devices, like wireless telephones, tablets and/or digital cameras. Thus, the warrant applied for would authorize the seizure of electronic storage media and electronic devices or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

11. I submit that if a computer and/or electronic devices are found on the target premises, there is probable cause to believe the records sought in this application will be stored on that computer and/or electronic device for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

12. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes



described on the warrant, but also forensic evidence that establishes how the computers and/or other electronic devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the computers and other electronic devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process.

Electronic evidence is not always data that can be merely reviewed by a review team and passed

along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

13. In most cases, a thorough search of a premises for information that might be stored on computers, electronic devices or other storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it

will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) as well as documentation, items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized or to activate specific equipment or software.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.



14. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

15. Based on my training and experience, I have probable cause to believe and I do believe, evidence from these crimes will be found at the target premises, or in the vehicles of Beth and Joseph Bing. The investigation indicates both Beth and Joseph Bing reside at the target premises based on information obtained from both the state of Maine and Unity College. It is my belief that evidence consisting of receipts, travel documentation to include but not limited to; airline tickets, rental car receipts, luggage tags, hotel receipts, and airport parking receipts. I further believe evidence associated with purchases made while on travel to include but not limited to Nike apparel, Michael Kors apparel, Coach apparel and other souvenirs would be located at the target premises.

16. The investigation has identified charges related to automobiles as well as an invoice located within the office of Beth Bing which would indicate the location of evidence showing how repairs were made for vehicles to include but not limited to auto tinting, safety inspections and automobile repairs.


17. It is my belief that items purchased through Amazon.com, Delta.com, Orbitz.com and greendot.com would have been made through the internet from electronic media and computing devices belonging to the Bings. This is the type of property that people commonly

keep in their home, and in the case of mobile computing devices, these items are frequently left in one's car. Even if these devices were not used to make the original purchase, any computing device used by Bethany Bing could contain emails relating to the purchases, or other information associating Bethany Bing with the accounts used to make the purchases. I therefore believe that evidence described in Attachment B will be located at the target premises, or in vehicles associated with Beth and Joseph Bing. It is further believed items purchased online would be delivered via a mail delivery service to the target premises, which is the only known location where Beth and Joseph Bing reside.

18. It is further my experience that mementos from travel would be located within the residence as well as documentation of casino winnings or losses. The investigation has identified numerous purchases from various retail establishments in Mashantucket, Connecticut utilizing the credit card of John Hopkins at the same time charges were made at the Foxwood Casino utilizing the credit card of Beth Bing. It is my belief Beth Bing utilized a card in her name and a card in the name of John Hopkins, without authority to purchase in excess of \$12,700.00 in the period of three days.

### **CONCLUSION**

Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the location described in Attachment A. I respectfully request that this Court issue a search warrant for the location described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

  
Raymond T. Goergen  
Special Agent  
Federal Bureau of Investigation

Sworn and subscribed before me this 5<sup>TH</sup> day of November, 2019

  
JOHN C. NIVISON  
UNITED STATES MAGISTRATE JUDGE